

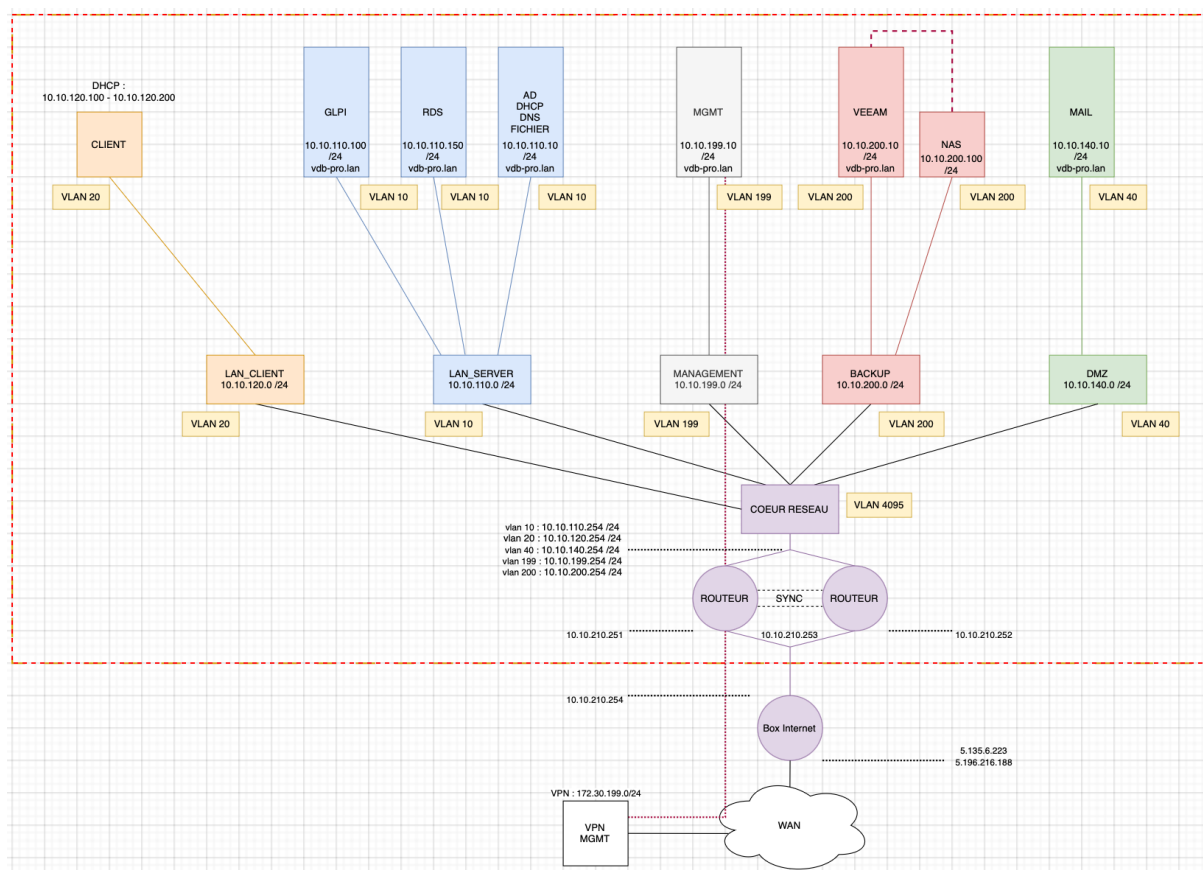
<p align="center">BTS Services informatiques aux organisations - SISR Session 2025</p>	
<p align="center">E6 – Support et mise à disposition de services informatiques Coefficient 4</p>	
<p align="center">DESCRIPTION DE LA REALISATION PROFESSIONNELLE</p>	
<p>NOM et prénom du candidat : Nathan VANDENBOSSCHE</p>	
<p>Contexte de la réalisation professionnelle</p> <ul style="list-style-type: none"> - Layer Bureautique et Informatique est une entreprise spécialisée dans la gestion d'infrastructures IT et la virtualisation, offrant des services essentiels pour répondre aux besoins de performance, sécurité et continuité des systèmes informatiques du client vdb-pro. - La problématique principale réside dans le besoin fondamental d'un service de messagerie fiable, permettant aux utilisateurs de communiquer efficacement par courriel au sein de l'organisation. Ce service doit offrir à la fois sécurité, continuité et facilité d'intégration avec les outils internes de l'entreprise. - La solution choisie consiste à mettre en place un serveur de messagerie Exchange, reconnu pour sa robustesse et sa capacité à gérer de manière centralisée les courriels, les calendriers et les contacts. Cette solution permettra également de bénéficier d'une gestion simplifiée et d'une intégration étroite avec Active Directory. 	
<p>Intitulé de la réalisation professionnelle Déploiement d'une Solution de Messagerie via Exchange</p>	
<p>Période de réalisation : 17/02/25 - 20/02/2025 Lieu : Auxerre</p> <p>Modalité : <input checked="" type="checkbox"/> Individuelle <input type="checkbox"/> En équipe</p>	
<p>Principale(s) activité(s) concernée(s) :</p> <ul style="list-style-type: none"> ○ METTRE A DISPOSITION DES UTILISATEURS UN SERVICE INFORMATIQUE ○ GERER LE PATRIMOINE INFORMATIQUE ○ ORGANISER SON DEVELOPPEMENT PROFESIONNEL ○ DEVELOPPER LA PRESENCE EN LIGNE DE L'ORGANISATION 	
<p>Conditions de réalisation</p> <ul style="list-style-type: none"> - Ressources disponibles (Situation avant RP) Nous disposons d'un serveur ESXi, une infrastructure fonctionnelle comprenant un Active Directory avec un service DNS fonctionnel, ainsi que d'un domaine public configuré pour l'entreprise. - Résultats attendus (Situation après RP) Une solution de messagerie Exchange fonctionnelle et sécurisée, permettant à l'ensemble des utilisateurs de communiquer par courriel électronique de manière fiable et protégée. - Durée de réalisation La mise en place de la solution a duré environ 4 jours, incluant les réunions, le temps nécessaire à l'installation du serveur et à la recherche d'informations pertinentes pour la configuration. 	
<p>Modalités d'accès à cette réalisation professionnelle.</p> <p>https://portfolio.vdb-pro.fr mdp : Cyb3r-M@P89\$</p>	

Partie 1 – Procédure de mise en œuvre

Dans le cadre de l'infrastructure personnelle que j'ai mise en place pour l'entreprise **vdb-pro**, j'ai conçu un environnement réseau complet intégrant un service de messagerie basé sur un serveur **Microsoft Exchange 2019**. Ce serveur permet aux utilisateurs de l'entreprise d'envoyer et de recevoir des courriels de manière sécurisée, tout en assurant la fiabilité des communications internes et externes.

Il offrira également un accès à une interface web sécurisé par un certificat, permettant la consultation des messages à distance via un simple navigateur internet.

La gestion des comptes utilisateurs et des droits d'accès à ce service de messagerie sera assurée par **l'Active Directory**, préalablement mis en place dans le cadre d'une autre Réalisation Professionnelle. Cela garantit une centralisation de l'authentification et une meilleure gestion des ressources au sein de l'organisation.



Mise en place d'une machine virtuelle

Dans le cadre de la mise en œuvre d'un service de messagerie via Microsoft Exchange Server 2019, une machine virtuelle dédiée a été provisionnée. Cette VM repose sur le système d'exploitation **Windows Server 2022**, et ses ressources ont été ajustées en fonction des recommandations Microsoft et des contraintes de la maquette.

Configuration recommandée par Microsoft :	Configuration utilisée dans la maquette :
Système d'exploitation : <ul style="list-style-type: none">- Windows Server 2022	Système d'exploitation : <ul style="list-style-type: none">- Windows Server 2022
Mémoire vive (RAM) : <ul style="list-style-type: none">- 16 Go	Mémoire vive (RAM) : <ul style="list-style-type: none">- 10 Go
Processeur : <ul style="list-style-type: none">- 4 vCPU	Processeur : <ul style="list-style-type: none">- 4 vCPU
Stockage : <ul style="list-style-type: none">- Volume NTFS pour le système- Volume NTFS ou ReFS pour la BDD	Stockage : <ul style="list-style-type: none">- Volume NTFS 100 Go OS- Volume ReFS 100Go BDD

Remarque : Exchange Server prend en charge les volumes formatés en **NTFS** ou **ReFS** selon l'usage. Toutefois, **ReFS ne peut pas être utilisé** pour les fichiers binaires ou l'installation du système.

Exigences en termes d'espace disque

D'après la documentation officielle de Microsoft, les prérequis en matière d'espace disque sont les suivants :

- Minimum **30 Go** d'espace libre sur la partition d'installation d'Exchange
- Minimum **200 Mo** libres sur la partition système
- Minimum **500 Mo** libres sur la partition dédiée à la base de données de file d'attente
- Il est toutefois recommandé de prévoir un espace **beaucoup plus conséquent** pour les bases de données, en fonction du nombre d'utilisateurs et de l'usage de la messagerie.

Préparation DNS et intégration au domaine

Preparation du DNS publique

Afin d'assurer la résolution correcte du serveur Exchange, les enregistrements DNS suivants doivent être configurés sur le fournisseur du domaine public :

Type	Nom DNS	Valeur	Priorité
A	webmail.vdb-pro.fr	5.196.216.188	-
CNAME	autodiscover.vdb-pro.fr	webmail.vdb-pro.fr	-
MX	@	webmail.vdb-pro.fr	10
SFP	@	v=spf1 mx ip4:5.196.216.188 include:mx.ovh.com -all	

<input type="checkbox"/>	webmail.vdb-pro.fr.	0	A	5.196.216.188	⋮
<input type="checkbox"/>	autodiscover.vdb-pro.fr.	0	CNAME	webmail.vdb-pro.fr.	⋮
<input type="checkbox"/>	vdb-pro.fr.	0	MX	10 webmail.vdb-pro.fr.	⋮

Preparation du DNS interne

Afin que la résolution de noms en interne se fasse correctement, sans passer par Internet ni créer une boucle de résolution, j'ai dû ajouter manuellement les entrées DNS correspondantes dans le serveur DNS de l'entreprise.

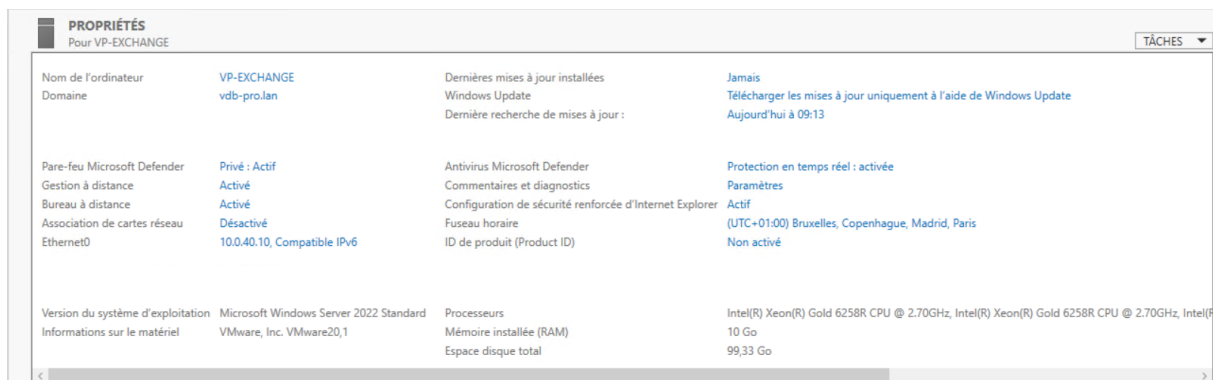
	Nom	Type	Données	Horodateur
DNS ▼ VP-DC1 Zones de recherche direc > _msdcs.vdb-pro.lan > vdb-pro.lan vdb-pro.fr Zones de recherche inver Points d'approbation Redirecteurs conditionne	(identique au dossier parent)	Source de nom (SOA)	[1], vp-dc1.vdb-pro.lan., ho...	statique
	(identique au dossier parent)	Serveur de noms (NS)	vp-dc1.vdb-pro.lan.	statique
	webmail	Alias (CNAME)	VP-EXCHANGE.vdb-pro.lan	
	autodiscover	Alias (CNAME)	webmail.vdb-pro.fr	

Cette configuration est essentielle pour garantir que les services, tels que le Webmail ou l'autodiscover d'Exchange, soient accessibles localement sans dépendre de la résolution externe. Cela permet non seulement de réduire la latence, mais aussi de mieux contrôler et sécuriser les flux réseau internes, tout en évitant des requêtes DNS inutiles vers l'extérieur.

Pour vérifier ces enregistrements, les commandes PowerShell suivantes peuvent être utilisées
Resolve-DnsName -Type A webmail.vdb-pro.fr | ft -AutoSize
Resolve-DnsName -Type MX vdb-pro.fr | ft -AutoSize

Le serveur Exchange doit également :

- Être **membre du domaine Active Directory** (commande : Add-Computer - DomainName vdb-pro.lan)
- Avoir une **forêt Active Directory** avec un niveau fonctionnel **Windows Server 2012 R2** minimum (Get-ADForest | fl Name,ForestMode)
- Être utilisé avec **Microsoft Outlook 2013** minimum pour garantir la compatibilité avec Exchange 2019



Préparation Firewall

En amont, une règle a été configurée afin de rediriger l'ensemble des flux en provenance de l'IP publique 5.196.216.188 vers mon routeur ayant l'adresse IP interne 10.10.210.253. Grâce à cette configuration, tous les flux sont désormais acheminés vers mon pare-feu PfSense.

Pour commencer, j'ai mis en place des redirections de ports via des règles NAT (Port Forwarding). Les règles sont automatiquement ajoutées dans la section WAN de PfSense, ce qui permet d'autoriser les flux entrants en fonction des services que l'on souhaite exposer.

Firewall / NAT / Port Forward
















Port Forward

1:1

Outbound

NPt

Rules

<input type="checkbox"/>		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	25 (SMTP)	VP_EXCHANGE	25 (SMTP)		  
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	443 (HTTPS)	VP_EXCHANGE	443 (HTTPS)		  
<input type="checkbox"/>	 	WAN	TCP	*	*	WAN address	80 (HTTP)	VP_EXCHANGE	80 (HTTP)		  

Firewall / Rules / WAN

Floating

WAN

LAN

VLANSERVER

VLANCLIENT

































VLANDMZ

VLANMGMT

VLANBACKUP

OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	 	22/47.15 MiB	IPv4 TCP	*	*	VP_EXCHANGE	443 (HTTPS)	*	none		NAT	     
<input type="checkbox"/>	 	0/493 KiB	IPv4 TCP	*	*	VP_EXCHANGE	80 (HTTP)	*	none		NAT	     
<input type="checkbox"/>	 	0/13 KiB	IPv4 TCP	*	*	VP_EXCHANGE	25 (SMTP)	*	none		NAT	     
<input type="checkbox"/>	 	0/2.28 MiB	IPv4 *	*	*	*	*	*	none		block any	     

Enfin, je vais définir les règles nécessaires pour gérer les flux sortants depuis le réseau LAN DMZ où se trouve mon serveur Exchange, afin d'assurer une communication sécurisée.

Firewall / Rules / VLANDMZ

Floating

WAN

LAN

VLANSERVER

VLANCLIENT

VLANDMZ

VLANMGMT

VLANBACKUP

OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 ICMP any	*	*	*	*	*	none			
<input type="checkbox"/>	0/2.44 GiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		HTTPS	
<input type="checkbox"/>	0/22.52 MiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none		HTTPS	
<input type="checkbox"/>	0/0 B	IPv4 TCP/UDP	AD_to_EXCHANGE	*	AD_to_EXCHANGE	*	*	none			
<input type="checkbox"/>	0/70 KiB	IPv4 TCP/UDP	VP_EXCHANGE	*	*	Mail	*	none		MAIL	
<input type="checkbox"/>	0/943 KiB	IPv4 *	*	*	*	*	*	none			

Installation des composants prérequis

Avant de procéder à l'installation d'Exchange Server, certains composants doivent être installés sur le serveur.

A. .NET Framework 4.8

Déjà installé par défaut sur Windows Server 2022. Si besoin, il est téléchargeable depuis le site Microsoft.

B. Visual C++ Redistributable Packages

- Visual Studio 2012
- Visual Studio 2013

Ces packages sont nécessaires au bon fonctionnement d'Exchange.

C. Unified Communications Managed API (UCMA) 4.0

Ce runtime est indispensable au fonctionnement de certains services Exchange. Il peut être téléchargé directement depuis Microsoft.

D. Fonctionnalités Windows à installer via PowerShell

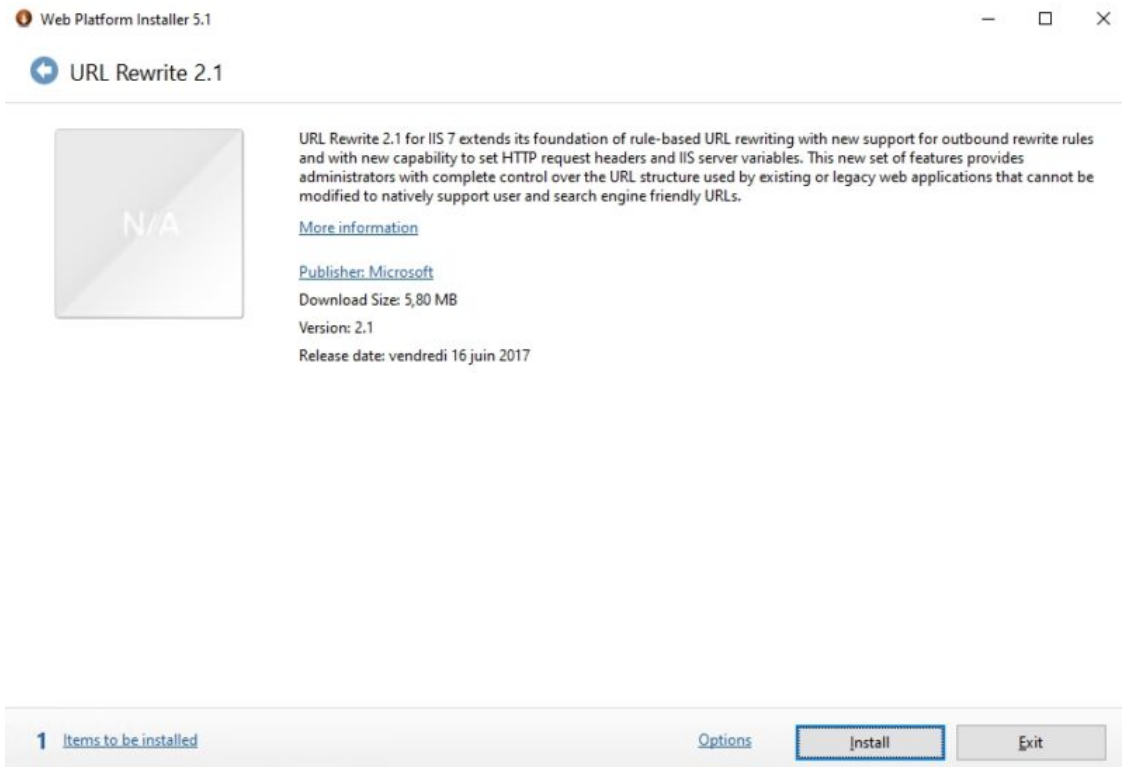
Voici la commande à exécuter pour installer l'ensemble des rôles et fonctionnalités nécessaires :

```
Install-WindowsFeature Server-Media-Foundation, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, RSAT-ADDS
```

Cette commande installe notamment IIS (nécessaire pour le Webmail) et d'autres services liés à l'administration, aux protocoles de communication et à la sécurité.

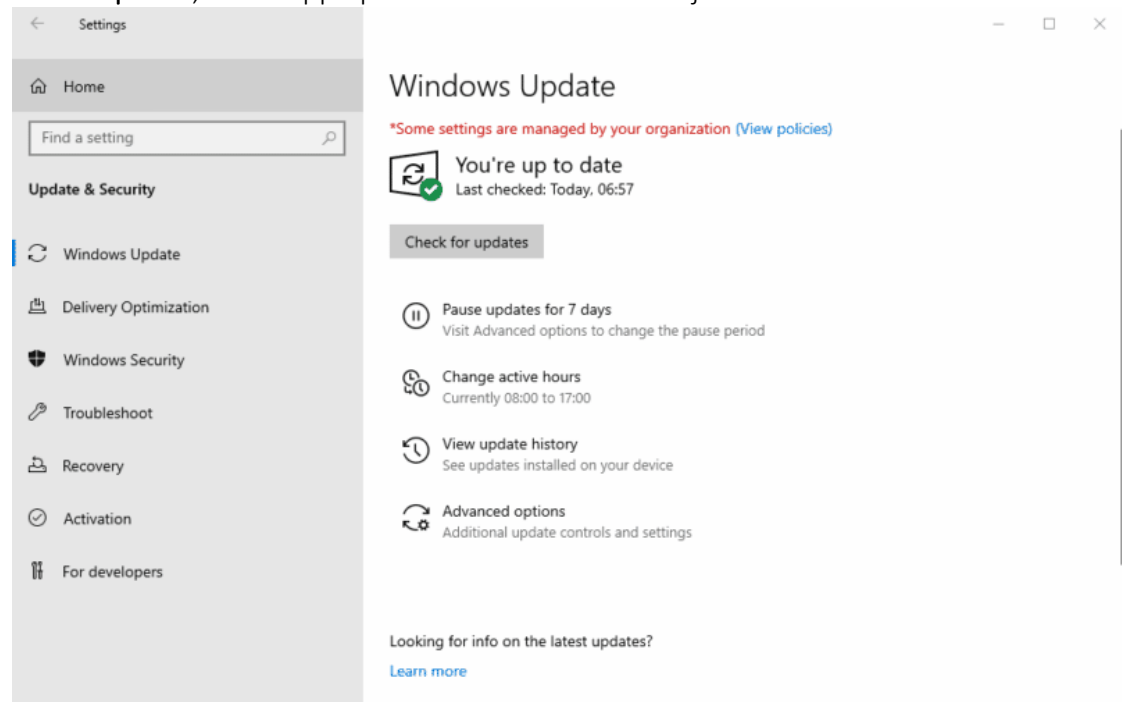
E. Installation du module URL Rewrite 2.1

Ce module est requis pour le bon fonctionnement d'Outlook Web Access (OWA) via le serveur IIS. Il est à installer manuellement.



F. Mise à jour du système

Avant de lancer l'installation d'Exchange Server, il est impératif de mettre à jour le système via **Windows Update**, afin d'appliquer les dernières mises à jour cumulatives.



Une fois l'ensemble des prérequis installés et correctement configurés sur le serveur, celui-ci est prêt à accueillir le service de messagerie Microsoft Exchange.

Dans ce cadre, j'ai réalisé un résumé structuré des étapes clés de l'installation d'Exchange Server 2019, en mettant en avant les points essentiels à retenir pour assurer une mise en œuvre réussie.

Installation de Microsoft Exchange Server 2019

Préparation avant installation

Avant de débiter l'installation d'Exchange Server 2019, il est impératif de :

- Se connecter au serveur avec un **compte membre du groupe "Administrateurs du domaine"**
- **Redémarrer le serveur** pour s'assurer qu'aucune mise à jour en attente n'interfère avec l'installation

Téléchargement et montage de l'ISO

L'installation nécessite de télécharger l'image ISO officielle d'Exchange. Dans cette maquette, l'installation est réalisée à partir de **Microsoft Exchange Server 2019 – Cumulative Update 15**.

- Lien officiel de téléchargement : [Microsoft Exchange Server 2019 CU15](#)
- Taille du fichier ISO : environ **5,8 Go**

Une fois le fichier téléchargé :

1. **Monter l'image ISO** (clic droit > Monter)
2. Exécuter le fichier setup.exe **en tant qu'administrateur**

Démarrage de l'assistant d'installation

Étapes initiales :

- Sélectionner l'option **"Connect to the Internet and check for updates"** afin de vérifier la présence de mises à jour plus récentes
- Attendre la fin de la phase **"Copying files"**
- Poursuivre jusqu'à l'étape d'**Introduction**, puis accepter les termes du contrat de licence

Choix des rôles :

- Sélectionner le **"Mailbox role"** (boîte aux lettres), rôle principal pour les services Exchange
- L'option **"Automatically install Windows Server roles and features..."** peut être décochée car les prérequis ont déjà été installés en amont via PowerShell

Répertoire d'installation :

L'installation par défaut se fait sur le disque [C:\] et nécessite environ **5,7 Go d'espace disponible**

The screenshot shows the 'Installation Space and Location' window of the Microsoft Exchange Server 2019 Cumulative Update 12 installer. At the top, the title bar reads 'MICROSOFT EXCHANGE SERVER 2019 CUMULATIVE UPDATE 12'. The main heading is 'Installation Space and Location'. Below this, it displays 'Disk space required: 5709,4 MB' and 'Disk space available: 109667,1 MB'. A section titled 'Specify the path for the Exchange Server installation:' contains a text box with the default path 'C:\Program Files\Microsoft\Exchange Server\V15' and a 'browse' button. At the bottom left is the 'Exchange' logo. At the bottom right are 'back' and 'next' buttons, with an orange arrow pointing to the 'next' button.

Configuration de l'organisation

- **Nom de l'organisation Exchange** : à personnaliser (ex. : nom de l'entreprise ou de la maquette)



The screenshot shows the 'Organisation Exchange' step of the Microsoft Exchange Server 2019 installation wizard. The title bar reads 'MICROSOFT EXCHANGE SERVER 2019 MISE À JOUR CUMULATIVE 15'. The main heading is 'Organisation Exchange'. Below it, a text prompt says 'Spécifiez le nom de cette organisation Exchange :'. A text box contains the value 'vdb-pro'. Below the text box is a checkbox labeled 'Appliquer le modèle de sécurité des autorisations partagées Active Directory à l'organisation Exchange'. A paragraph explains that this model is for large organizations separating Exchange and Active Directory responsibilities, and that it prevents creating Active Directory objects like users, groups, and contacts. Below this, a note states that the model should not be applied if the same person or group manages both Exchange and Active Directory, with a link to <https://aka.ms/ADSplitPermissions> for more information. At the bottom, a list item indicates that the 'Apply Active Directory split permissions security model' option should be left **désactivée** (disabled) if the same administrator manages both.

MICROSOFT EXCHANGE SERVER 2019 MISE À JOUR CUMULATIVE 15

Organisation Exchange

Spécifiez le nom de cette organisation Exchange :

vdb-pro

☐ Appliquer le modèle de sécurité des autorisations partagées Active Directory à l'organisation Exchange

Le modèle de sécurité d'autorisations partagées Active Directory est généralement utilisé par les grandes organisations qui séparent les responsabilités de gestion d'Exchange et d'Active Directory en différents groupes de personnes. L'application de ce modèle de sécurité empêche les administrateurs et serveurs Exchange de créer des objets Active Directory, tels que des utilisateurs, des groupes et des contacts. La possibilité de gérer des attributs non Exchange sur ces objets est également supprimée.

Vous ne devez pas appliquer ce modèle de sécurité si la même personne ou le même groupe gère Exchange et Active Directory. Cliquez sur <https://aka.ms/ADSplitPermissions> pour plus d'informations.

- Option "Apply Active Directory split permissions security model" : laisser **désactivée** si le même administrateur gère Active Directory et Exchange

Une fois ces points validés :

- Cliquer sur **"Install"** pour démarrer l'installation
- **Durée approximative** : 30 minutes à 1 heure, en fonction des ressources de la machine

Fin de l'installation




















Une fois l'installation terminée :

- **Redémarrer le serveur** pour finaliser le processus

Conséquences de l'installation

À l'issue de l'installation, une nouvelle **Unité d'Organisation (OU)** est automatiquement créée dans Active Directory :

- **Microsoft Exchange Security Groups**
- Elle contient l'ensemble des **groupes d'administration** nécessaires à la gestion du serveur Exchange (droits, délégations, sécurité, etc.)

Name	Type	Description
 Compliance Management	Security Group - Universal	This role group will allow a specified user, responsible for complianc
 Delegated Setup	Security Group - Universal	Members of this management role group have permissions to instal
 Discovery Management	Security Group - Universal	Members of this management role group can perform searches of n
 Exchange Servers	Security Group - Universal	This group contains all the Exchange servers. This group shouldn't b
 Exchange Trusted Subsystem	Security Group - Universal	This group contains Exchange servers that run Exchange cmdlets on
 Exchange Windows Permissions	Security Group - Universal	This group contains Exchange servers that run Exchange cmdlets on
 ExchangeLegacyInterop	Security Group - Universal	This group is for interoperability with Exchange 2003 servers within t
 Help Desk	Security Group - Universal	Members of this management role group can view and manage the
 Hygiene Management	Security Group - Universal	Members of this management role group can manage Exchange an
 Managed Availability Servers	Security Group - Universal	This group contains all the Managed Availability servers. This group
 Organization Management	Security Group - Universal	Members of this management role group have permissions to mana
 Public Folder Management	Security Group - Universal	Members of this management role group can manage public folder
 Recipient Management	Security Group - Universal	Members of this management role group have rights to create, man
 Records Management	Security Group - Universal	Members of this management role group can configure compliance
 Security Administrator	Security Group - Universal	Membership in this role group is synchronized across services and n
 Security Reader	Security Group - Universal	Membership in this role group is synchronized across services and n
 Server Management	Security Group - Universal	Members of this management role group have permissions to mana
 UM Management	Security Group - Universal	Members of this management role group can manage Unified Mess
 View-Only Organization Management	Security Group - Universal	Members of this management role group can view recipient and coi

Première utilisation d'Exchange

Centre d'administration Exchange et Exchange Management Shell

L'administration d'Exchange s'effectue au travers d'un portail d'administration en mode Web, ainsi que de commandes PowerShell. Le portail d'administration appelé "Centre d'administration Exchange" est accessible à cette adresse :

# En local sur le serveur https://localhost/ecp	# À partir d'une machine du réseau local https://vp-exchange/ecp	# À partir de l'extérieur https://webmail.vdb-pro.fr/ecp
--	---	--

Sur cette interface, vous pouvez vous authentifier avec un compte administrateur du domaine.

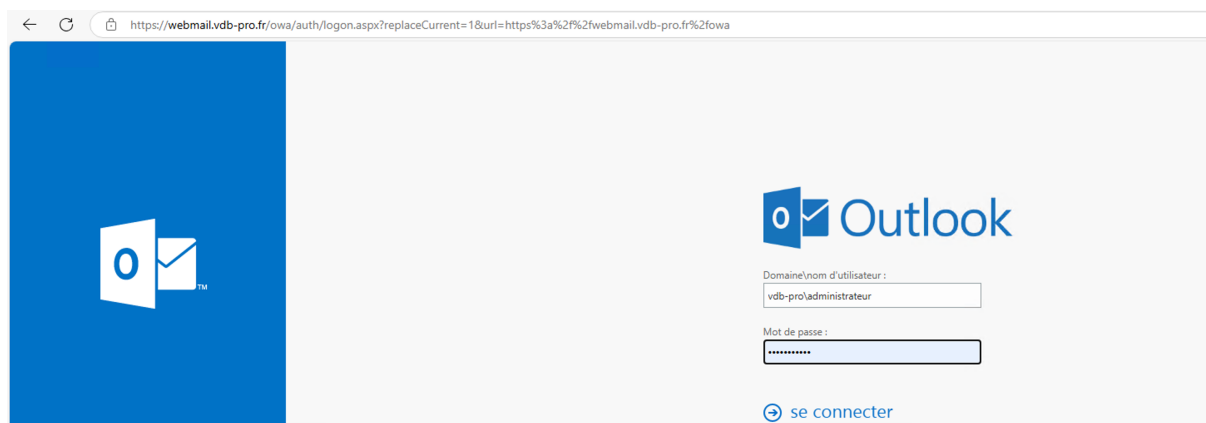


Webmail d'Exchange Server 2019

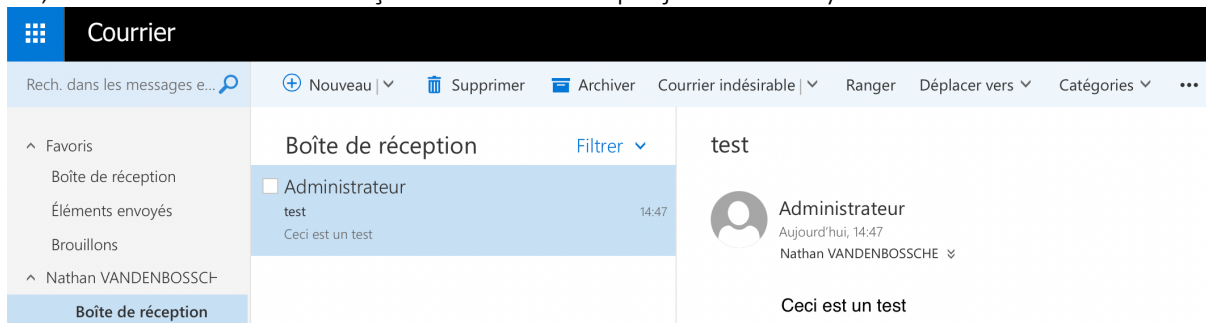
En ce qui concerne les utilisateurs, ils ont le choix entre un client de messagerie type Outlook, ou un accès via le webmail. Ce dernier étant accessible à l'adresse suivante :

<https://webmail.vdb-pro.fr/owa>

Le sigle "OWA" fait référence à Outlook Web Access. L'utilisateur doit se connecter avec ses identifiants Active Directory (*au préalable, j'ai créé les BAL*).



Ah, mon utilisateur a bien reçu l'e-mail de test que je lui ai envoyé !



Déplacer la base de données Exchange

Suite à l'installation de Microsoft Exchange, je constate que la base de données (au format EDB) et les journaux sont initialement stockés dans l'emplacement par défaut, à côté des binaires d'Exchange : C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 0780012571\Mailbox Database 0780012571.edb

Il est toutefois recommandé de déplacer cette base de données sur un autre volume, tout comme les journaux, afin d'optimiser les performances et la gestion des données. Dans un environnement de production, il est préférable d'utiliser au moins deux volumes distincts : un pour la base de données et un autre pour les journaux. Dans mon cas, je vais profiter du fait que le serveur vient juste d'être installé, ce qui rend cette opération relativement simple et rapide à effectuer.

Mon objectif ici est de déplacer la base de données et les journaux vers un volume ReFS (Resilient File System) pour bénéficier d'une meilleure intégrité des données et de performances accrues. Le chemin que j'ai choisi pour ce déplacement est le suivant : E:\MsExchange_DB\

En même temps, je vais renommer la base de données. En effet, le nom par défaut, "Mailbox Database 0780012571.edb", n'est pas particulièrement explicite. Je préfère attribuer un nom plus pertinent, à savoir "Mailbox vdb-pro", afin de faciliter la gestion à long terme.

Pour ce faire, je vais d'abord ouvrir l'Exchange Management Shell. Ensuite, je lance la commande suivante pour renommer la base de données :

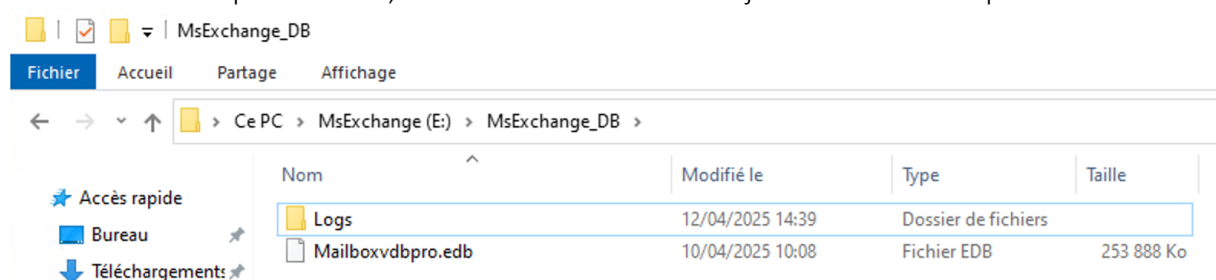
```
Get-MailboxDatabase "Mailbox Database 0780012571" | Set-MailboxDatabase -Name "Mailbox IT-Connect"
```

Ensuite, je passe à l'étape suivante : déplacer la base de données et les journaux vers leur nouvel emplacement. Pour cela, j'utilise la commande Move-DatabasePath :

```
Move-DatabasePath "Mailbox vdb-pro" -EdbFilePath "E:\MsExchange_DB\Mailboxvdbpro.edb" -LogFolderPath "E:\MsExchange_DB\Logs\"
```

L'opération est relativement rapide, mais il est important de noter que pendant cette opération, la base de données sera temporairement indisponible.

Une fois cette étape terminée, ma base de données et ses journaux seront déplacés avec succès



Créer une nouvelle boîte aux lettres Exchange

Pour créer une boîte aux lettres (*appelée aussi "BAL"*) pour un utilisateur, Je commence par me rendre dans le menu **Destinataire** puis **Boîtes aux lettres**. Une fois sur cette page, je clique sur le bouton "+" pour ajouter une nouvelle boîte aux lettres.

Dans ce formulaire, j'ai le choix entre **sélectionner un utilisateur existant** dans l'annuaire Active Directory ou **créer un utilisateur** en même temps que la boîte aux lettres. Il est important de souligner que dans Exchange, les comptes utilisateurs et les boîtes aux lettres sont étroitement liés. Cela signifie que lorsque je crée une boîte aux lettres pour un utilisateur, celle-ci est directement associée à son compte dans Active Directory.

Je dois également garder à l'esprit un aspect crucial : si je **supprime une boîte aux lettres** dans Exchange, l'utilisateur associé dans Active Directory sera également **supprimé**. Cela peut avoir des conséquences importantes, car cela supprimera non seulement la boîte aux lettres, mais également l'accès de l'utilisateur à son compte AD. Il est donc primordial d'être vigilant lors de la gestion de ces boîtes aux lettres.

The screenshot displays the Exchange Admin Center (EAC) interface. The top navigation bar includes the Office 365 logo and the text 'ENTREPRISE Office 365'. The main header is 'Centre d'administration Exchange'. On the left, a sidebar lists various management areas: 'destinataires' (selected), 'autorisations', 'gestion de la conformité', 'organisation', 'protection', 'flux de courrier', 'mobile', 'dossiers publics', 'serveurs', and 'hybride'. The main content area is titled 'boîtes aux lettres' and includes sub-links for 'groupes', 'ressources', 'contacts', and 'boîte aux lettres par'. The 'nouvelle boîte aux lettres utilisateur' form is shown, with a browser window title 'Boîte aux lettres utilisateur - Profile 1 - Microsoft Edge' and a 'Not secure' warning. The form contains fields for 'Alias', 'Prénom', 'Initiales', and 'Nom'. It also has radio buttons for 'Utilisateur existant' (selected) and 'Nouvel utilisateur', and a 'Parcourir...' button. A tooltip explains that the alias is the part of the email address before the '@' symbol and must be unique.

ENTREPRISE Office 365

Centre d'administration Exchange

destinataires

boîtes aux lettres groupes ressources contacts boîte aux lettres par

Boîte aux lettres utilisateur - Profile 1 - Microsoft Edge

Not secure | <https://localhost/ecp/UsersGroups/NewMailb...>

nouvelle boîte aux lettres utilisateur

Alias :

Utilisateur existant

Parcourir...

Nouvel utilisateur

Prénom :

Initiales :

Nom :

L'alias de l'utilisateur est la partie de l'adresse de courrier située à gauche du symbole @. Il doit être unique dans votre organisation.

Ajout d'un domaine et strategie d'adresse de courrier

Actuellement mon serveur Exchange est installé sur un domaine Active Directory avec un domaine non routable (vdb-pro.lan) je rencontre une situation où le domaine de l'adresse e-mail interne ne correspondra pas à celui utilisé pour la communication avec l'extérieur.

En effet, les domaines non routables (tels que ".local" ou ".lan") ne sont pas accessibles via Internet, ce qui pose un problème pour l'envoi ou la réception d'emails en dehors du réseau interne. Par conséquent, je dois configurer un domaine différent dans Exchange, qui sera routable et capable de communiquer avec l'extérieur.

Pour cela, je vais d'abord déclarer ce nouveau domaine dans Exchange. Ensuite, je l'associe à une politique d'adresses e-mails pour que les utilisateurs de mon serveur Exchange puissent recevoir et envoyer des emails en utilisant ce domaine public.

Centre d'administration Exchange

destinataires autorisations gestion de la conformité organisation protection **flux de courrier** mobile dossiers publics serveurs hybride

règles rapports de remise **domaines acceptés** stratégies d'adresse de courrier connecteurs de réception connecteurs d'envoi

NOM	DOMAINE ACCEPTÉ	TYPE DE DOMAINE
vdb-pro.fr	vdb-pro.fr	Faisant autorité
vdb-pro.lan (domaine par défaut)	vdb-pro.lan	Faisant autorité

vdb-pro.fr

Nom de domaine complet : vdb-pro.fr
Type de domaine : Faisant autorité

Centre d'administration Exchange

destinataires autorisations gestion de la conformité organisation protection **flux de courrier** mobile dossiers publics serveurs hybride

règles rapports de remise domaines acceptés **stratégies d'adresse de courrier** connecteurs de réception connecteurs d'envoi

NOM	PRIORITÉ	ÉTAT
Default Policy	La plus faible	Appliqué

Default Policy

Format de l'adresse de courrier
SMTP
Principal :@vdb-pro.fr

Inclut
Tous les types de destinataire

Cette stratégie d'adresse de courrier a été appliquée.

Cette opération garantit que les adresses e-mails de mes utilisateurs auront un domaine valide et accessible de manière routable, ce qui est essentiel pour toute communication en dehors du réseau local. Cette étape est nécessaire pour assurer une connectivité correcte de mes utilisateurs Exchange avec l'extérieur, tout en préservant l'intégrité et l'accessibilité des boîtes aux lettres internes.

Une fois que c'est fait, je peux créer des boîtes aux lettres : par défaut, elles bénéficieront d'une adresse e-mail principale en "@vdb-pro.fr".

Ajout d'un certificat SSL pour Exchange

Une étape cruciale dans le processus de création d'un serveur de messagerie Exchange est l'ajout d'un certificat SSL/TLS.

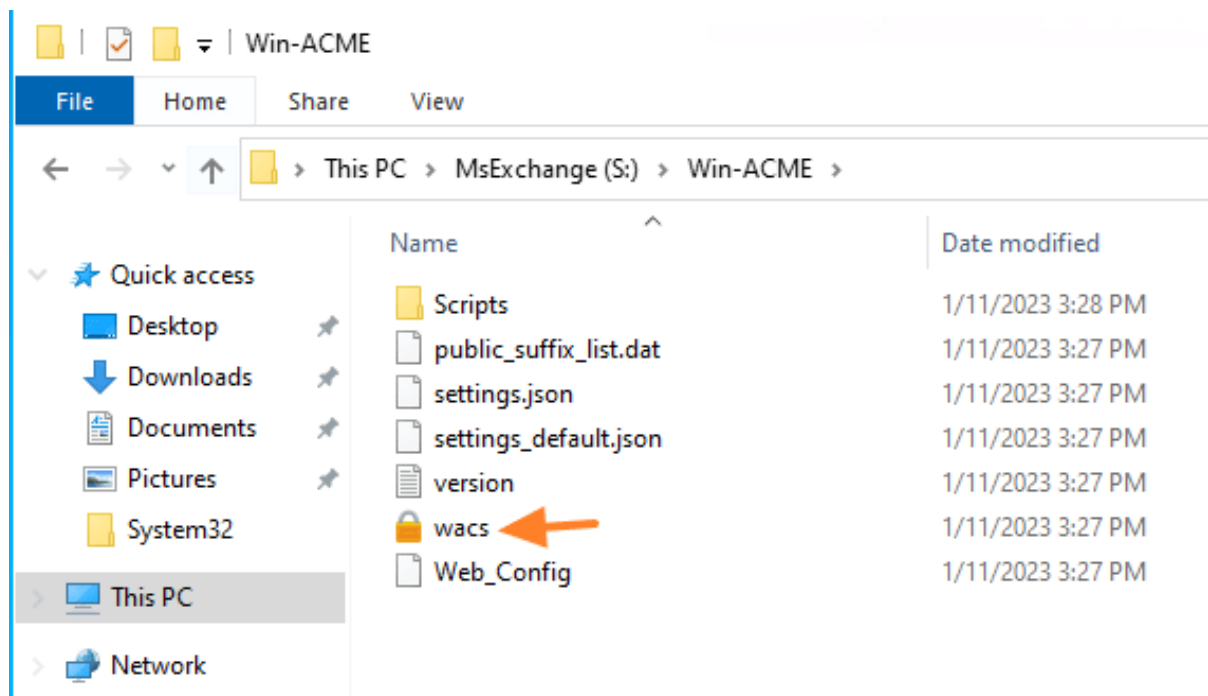
Ce certificat est essentiel pour garantir que mon serveur Exchange soit accessible en toute sécurité depuis l'extérieur, notamment pour les utilisateurs qui se connectent à distance via des clients de messagerie comme Outlook ou des applications mobiles. Le certificat assure que les communications entre les utilisateurs et le serveur Exchange sont cryptées, protégeant ainsi les données sensibles contre les interceptions.

Pour ce faire, je vais obtenir un certificat auprès d'une autorité de certification (CA) reconnue. Le certificat permet également d'éviter les avertissements de sécurité lorsque les utilisateurs se connectent à leur boîte aux lettres, renforçant ainsi la confiance et la sécurité de l'infrastructure de messagerie.

L'ajout de ce certificat est indispensable pour garantir une connexion sécurisée, conforme aux bonnes pratiques de sécurité et pour protéger l'intégrité des communications via Exchange.

Demander un certificat SSL avec Win-ACME

Je commence par télécharger le client Win-ACME, par extraire le contenu et exécuter en tant qu'administrateur "wacs.exe".



Bien qu'il soit possible d'effectuer une demande de certificat en ligne de commandes en précisant tous les arguments, nous allons procéder étape par étape, via le mode interactif. De ce fait, j'exécute "wacs.exe" en tant qu'administrateur et choisis l'option "M" correspondante à "Create certificate (full options)".

```
S:\Win-ACME\wacs.exe

A simple Windows ACMEv2 client (WACS)
Software version 2.1.23.1315 (release, pluggable, standalone, 64-bit)
Connecting to https://acme-v02.api.letsencrypt.org/...
Connection OK!
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (0 total)
O: More options...
Q: Quit

Please choose from the menu: M_
```

Je dois préciser les noms DNS à couvrir avec le certificat SSL. Pour cela, je sélectionne l'option "2" pour effectuer une saisie manuelle.

```
Running in mode: Interactive, Advanced

Please specify how the list of domain names that will be included in the
certificate should be determined. If you choose for one of the "all bindings"
options, the list will automatically be updated for future renewals to
reflect the bindings at that time.

1: Read bindings from IIS
2: Manual input
3: CSR created by another program
C: Abort

How shall we determine the domain(s) to include in the certificate?: 2_
```

Je vais ensuite indiquer toutes les adresses Web utilisées par mon serveur Exchange. Dans mon cas, il y en a deux : **webmail.vdb-pro.fr** et **autodiscover.vdb-pro.fr**. Je peux aussi indiquer un nom convivial pour le certificat, mais cela reste optionnel. Si je ne souhaite pas le faire, je peux simplement appuyer sur **Entrée** pour passer cette étape.

```
Description:      A host name to get a certificate for. This may be a
                  comma-separated list.

Host: webmail.vdb-pro.fr,autodiscover.vdb-pro.fr

Source generated using plugin Manual: webmail.vdb-pro.fr and 1 alternatives

Friendly name '[Manual] webmail.vdb-pro.fr'. <Enter> to accept or type desired name: <Enter>
```

Concernant la méthode de validation, je vais commencer par tester la méthode par défaut en sélectionnant l'option "2".

```

1: [http-01] Save verification files on (network) path
2: [http-01] Serve verification files from memory
3: [http-01] Upload verification files via FTP(S)
4: [http-01] Upload verification files via SSH-FTP
5: [http-01] Upload verification files via WebDav
6: [dns-01] Create verification records manually (auto-renew not possible)
7: [dns-01] Create verification records with acme-dns (https://github.com/joohoi/acme-dns)
8: [dns-01] Create verification records with your own script
9: [tls-alpn-01] Answer TLS verification request from win-acme
C: Abort

How would you like prove ownership for the domain(s)?: 2

```

Ensuite, je dois choisir le type de clé privée à utiliser. Dans ce cas, je sélectionne l'option "2" pour RSA Key, qui est la méthode la plus courante et recommandée.

```

After ownership of the domain(s) has been proven, we will create a
Certificate Signing Request (CSR) to obtain the actual certificate. The CSR
determines properties of the certificate like which (type of) key to use. If
you are not sure what to pick here, RSA is the safe default.

1: Elliptic Curve key
2: RSA key
C: Abort

What kind of private key should be used for the certificate?: 2

```

L'assistant me demande où je souhaite stocker le certificat. Pour cela, je choisis "4" afin qu'il soit stocké dans le magasin des certificats Windows. Lors de la question suivante, je dois indiquer le magasin où il sera stocké, et je sélectionne "2" pour le **magasin personnel**, ce qui est recommandé pour Exchange, selon les indications de l'assistant. Une fois cela fait, je sélectionne "5" pour passer à l'étape suivante, car il n'y a pas d'autres emplacements à spécifier.

```

1: IIS Central Certificate Store (.pfx per host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store
5: No (additional) store steps

How would you like to store the certificate?: 4

1: [WebHosting] - Dedicated store for IIS
2: [My] - General computer store (for Exchange/RDS)
3: [Default] - Use global default, currently WebHosting

Choose store to use, or type the name of another unlisted store: 2

1: IIS Central Certificate Store (.pfx per host)
2: PEM encoded files (Apache, nginx, etc.)
3: PFX archive
4: Windows Certificate Store
5: No (additional) store steps

Would you like to store it in another way too?: 5

```

Win-ACME me propose ensuite de mettre à jour les liaisons dans IIS pour intégrer le certificat SSL. Je confirme cette action en sélectionnant "1" une première fois, puis une seconde fois pour appliquer le certificat au niveau du site "Default Web Site" dans IIS.

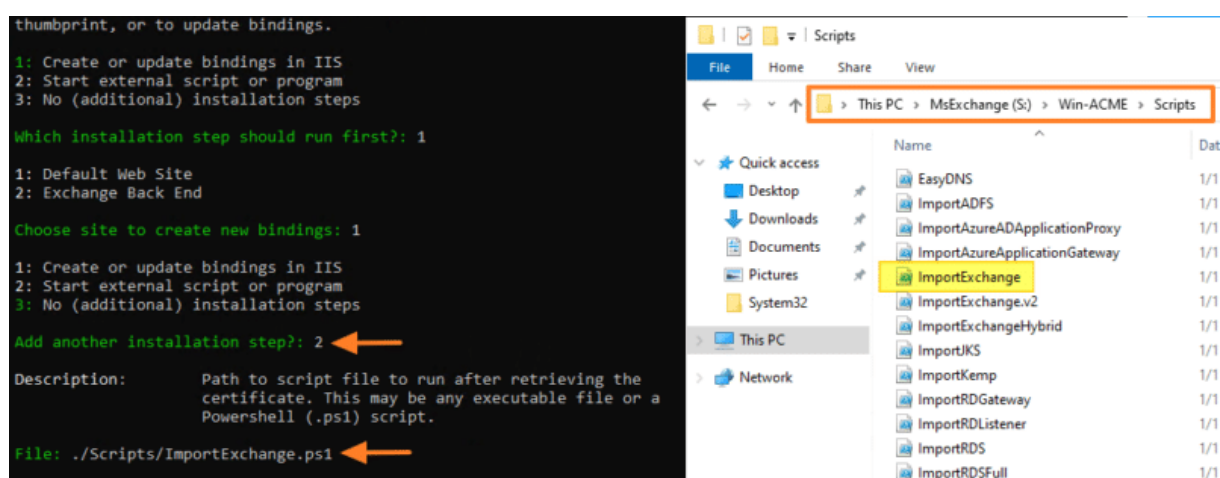
```
1: Create or update bindings in IIS
2: Start external script or program
3: No (additional) installation steps

Which installation step should run first?: 1

1: Default Web Site
2: Exchange Back End

Choose site to create new bindings: 1
```

L'assistant me demande ensuite si je souhaite ajouter une étape d'installation supplémentaire. Je réponds "oui" car je dois exécuter un script supplémentaire. Pour cela, je choisis "2", ce qui me permet de spécifier le chemin du script PowerShell intégré à Win-ACME, **ImportExchange.ps1**. Le chemin à entrer est : « ./Scripts/ImportExchange.ps1 »



Je vais ensuite préciser les paramètres nécessaires à l'exécution de ce script. Pour cela, je saisis les informations suivantes pour Microsoft Exchange Server :

'{CertThumbprint}' 'IIS,SMTP,IMAP' 1 '{CacheFile}' '{CachePassword}' '{CertFriendlyName}'

```
Parameters: '{CertThumbprint}' 'IIS,SMTP,IMAP' 1 '{CacheFile}' '{CachePassword}' '{CertFriendlyName}'
```

Une fois cela fait, je sélectionne "3" pour indiquer qu'il n'y a pas d'autres étapes d'installation à ajouter.

```
Parameters: '{CertThumbprint}' 'IIS,SMTP,IMAP' 1 '{CacheFile}' '{CachePassword}' '{CertFriendlyName}'  
1: Create or update bindings in IIS  
2: Start external script or program  
3: No (additional) installation steps  
Add another installation step?: 3
```

À partir de là, le client Win-ACME va émettre une requête pour obtenir le certificat SSL. Si la requête est acceptée, le certificat sera installé dans le magasin de certificats du serveur et IIS sera configuré pour utiliser ce certificat au sein des liaisons HTTPS. De plus, une tâche planifiée nommée **"win-acme renew (acme-v02.api.letsencrypt.org)"** sera créée sur le serveur pour assurer le renouvellement automatique du certificat, qui sera valable pour une durée de 90 jours à chaque renouvellement.

```
Plugin Manual generated source webmail.vdb-pro.fr with 2 identifiers  
Plugin Single created 1 order  
Cached order has status invalid, discarding  
[autodiscover.vdb-pro.fr] Authorizing...  
[autodiscover.vdb-pro.fr] Authorizing using http-01 validation (SelfHosting)  
[autodiscover.vdb-pro.fr] Authorization result: valid  
[webmail.vdb-pro.fr] Authorizing...  
[webmail.vdb-pro.fr] Authorizing using http-01 validation (SelfHosting)  
[webmail.vdb-pro.fr] Authorization result: valid  
Downloading certificate [Manual] webmail.vdb-pro.fr  
Store with CertificateStore...  
Installing certificate in the certificate store  
Adding certificate [Manual] webmail.vdb-pro.fr @ 2025/4/11 in store My  
Adding certificate Cn=Web, O=Let's Encrypt, C=US in store CA  
Installation step 1/2: IIS...  
Our best match was the default binding and it seems there are other non-SNI enabled bindings listening to the same endpoint, which means we cannot update it without po  
tentially causing problems. Instead, a new binding will be created. You may manually update the bindings if you want IIS to be configured in a different way.  
Our best match was the default binding and it seems there are other non-SNI enabled bindings listening to the same endpoint, which means we cannot update it without po  
tentially causing problems. Instead, a new binding will be created. You may manually update the bindings if you want IIS to be configured in a different way.  
Adding new https binding *:443:webmail.vdb-pro.fr  
Our best match was the default binding and it seems there are other non-SNI enabled bindings listening to the same endpoint, which means we cannot update it without po  
tentially causing problems. Instead, a new binding will be created. You may manually update the bindings if you want IIS to be configured in a different way.  
Our best match was the default binding and it seems there are other non-SNI enabled bindings listening to the same endpoint, which means we cannot update it without po  
tentially causing problems. Instead, a new binding will be created. You may manually update the bindings if you want IIS to be configured in a different way.  
Adding new https binding *:443:autodiscover.vdb-pro.fr  
Committing 2 https binding changes to IIS while updating site 1  
Installation step 2/2: Script...  
Script .\Scripts\ImportExchange.ps1 starting with parameters '3411f576A7A059C4F64B02F7B93116E68C71EA33' 'IIS,SMTP,IMAP' 1 'C:\ProgramData\win-acme\acme-v02.api.letsenc  
rypt.org\Certificates\QxI1fr-9d0KmbvxpPzZsw-main-e186e164a48b43e5c113c0c07e1c88339d0ec710-temp.pfx' '*****' '[Manual] webmail.vdb-pro.fr @ 2025/4/11'  
Script finished  
Adding Task Scheduler entry with the following settings  
- Name win-acme renew (acme-v02.api.letsencrypt.org)  
- Path C:\Users\Administrateur.VDB-PRO\Downloads\win-acme.v2.2.9.1701.x64.pluggable  
- Command wacs.exe --renew --baseurl "https://acme-v02.api.letsencrypt.org/"  
- Start at 00:00:00  
- Random delay 04:00:00  
- Time limit 02:00:00
```

Au final, mon serveur aura récupéré et installé le certificat SSL de Let's Encrypt, qui sera ensuite intégré à Exchange et IIS. La console me fournit des informations sur la tâche planifiée de renouvellement du certificat SSL. L'assistant me demande enfin si je souhaite exécuter cette tâche avec un utilisateur spécifique, et je réponds "no".

```
Do you want to specify the user the task will run as? (y/n*) - no  
Adding renewal for [Manual] webmail.vdb-pro.fr  
Next renewal due after 2025/6/5  
Certificate [Manual] webmail.vdb-pro.fr created
```

Vérification de la présence du certificat dans Exchange

À partir de ce moment, je peux me connecter à l'OWA (Webmail) d'Exchange pour vérifier que la connexion est bien sécurisée. En consultant les détails du certificat, je m'assure qu'il s'agit bien d'un certificat SSL valide de **Let's Encrypt**.

https://webmail.vdb-pro.fr/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fwebmail.vdb-pro.fr%2fowa%2f

Visionneuse de certificats : webmail.vdb-pro.fr

Général Détails

Émis pour

Nom commun (CN)	webmail.vdb-pro.fr
Organisation (O)	<Ne fait pas partie du certificat>
Unité d'organisation (UO)	<Ne fait pas partie du certificat>

Émis par

Nom commun (CN)	R10
Organisation (O)	Let's Encrypt
Unité d'organisation (UO)	<Ne fait pas partie du certificat>

Période de validité

Date d'émission	vendredi 11 avril 2025 à 08:18:20
Date d'expiration	jeudi 10 juillet 2025 à 08:18:19

Empreintes digitales SHA-256

Certificat	4877fd04c934fbc0df7a7b44d6e5858a89cb7b8d6c9f7f55d97515fe42602f50
Clé publique	949bfe967fad11822d628dd5c6d99d8cd9d00012291b97239751130532de961

Enfin, je peux vérifier la présence du certificat SSL dans le Centre d'administration Exchange, à l'emplacement suivant : **Serveurs > Certificats**.

https://webmail.vdb-pro.fr/ecp/?exsvurl=1&p=ReceiveConnectors

ENTREPRISE Office 365 Administrateur

Centre d'administration Exchange

destinataires serveurs bases de données groupes de disponibilité de la base de données répertoires virtuels **certificats**

Sélectionner le serveur : VP-EXCHANGE.vdb-pro.lan

+ / - / X / ...

NOM	STATUT	EXPIRE LE	
[Manual] webmail.vdb-pro.fr @ 2025/4/11	Valide	10/07/2025	<p>[Manual] webmail.vdb-pro.fr @ 2025/4/11</p> <p>Certificat signé par l'autorité de certification</p> <p>Émetteur : CN=R10, O=Let's Encrypt, C=US</p> <p>État</p> <p>Valide</p> <p>Expire le : 10/07/2025</p> <p>Renouveler</p> <p>Attribués aux services</p> <p>IMAP, IIS</p>
Microsoft Exchange Server Auth Certificate	Valide	14/03/2030	
Microsoft Exchange	Valide	09/04/2030	
WMSVC-SHA2	Valide	07/04/2035	

Protéger le centre d'administration

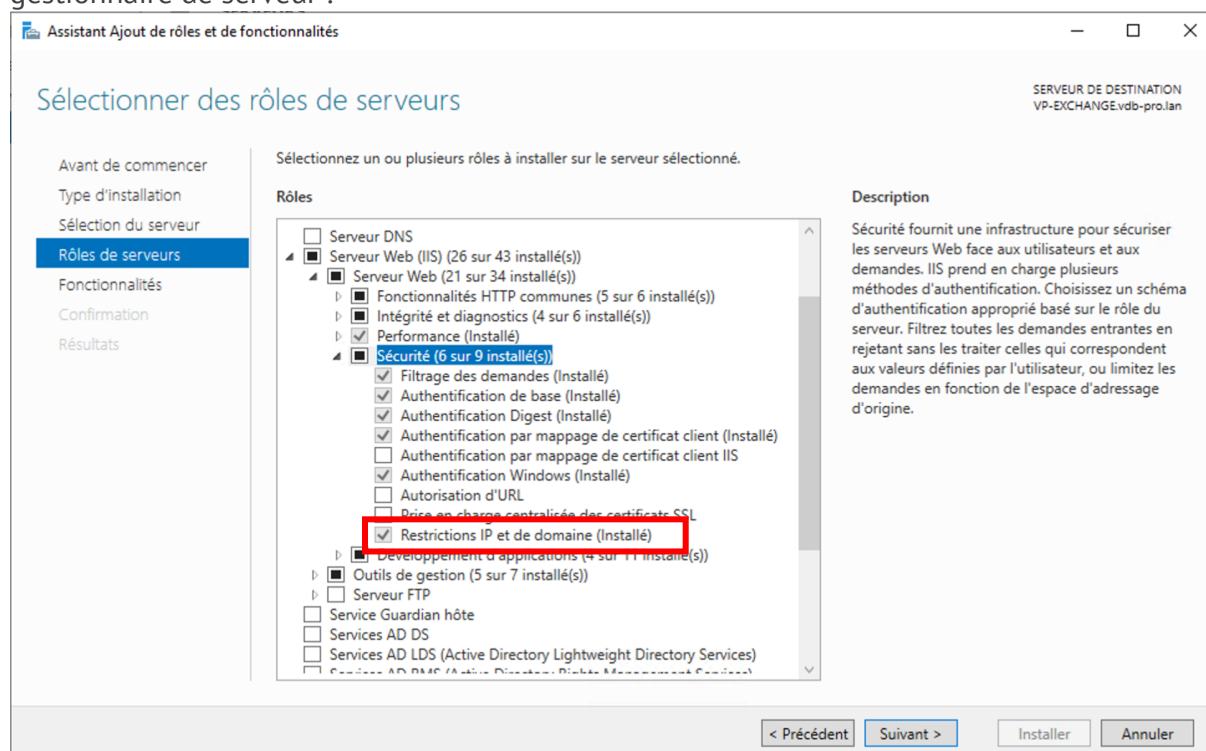
Je vous rappelle que par défaut, le Centre d'administration Exchange est accessible depuis le serveur Exchange en lui-même, depuis une machine du réseau local, mais aussi à partir d'Internet (si vous avez autorisé le flux HTTPS pour un accès au Webmail). Pour des raisons évidentes de sécurité, il est préférable de limiter l'accès à la console d'administration à partir de certaines adresses IP, ou au pire, à partir du réseau local. Il vaut mieux éviter que cette console soit accessible depuis l'extérieur.

Puisque le protocole HTTPS est utilisé aussi pour accéder au Webmail, nous ne pouvons pas jouer directement avec le pare-feu de Windows, car on couperait aussi l'accès au Webmail. La restriction doit être appliquée sur une couche supérieure, je vais configurer le serveur Web IIS grâce au module de restriction par adresses IP

Installer la fonction "Restrictions par adresse IP et domaine"

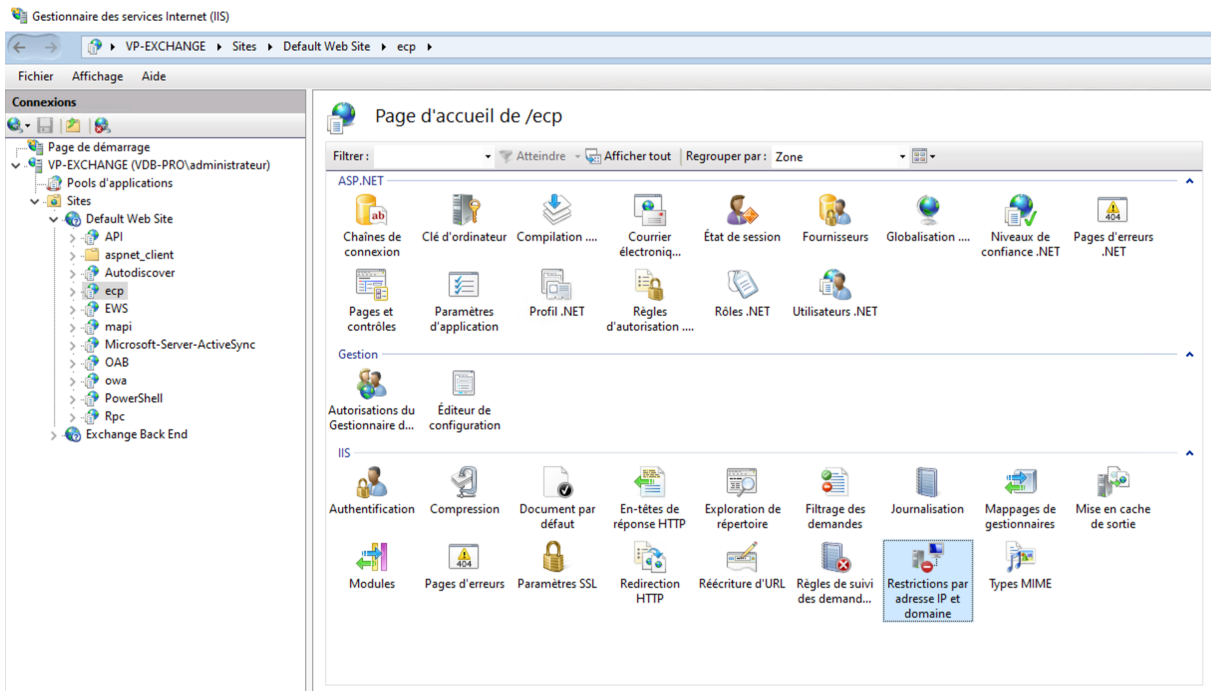
Sur votre serveur Exchange, dégainez la console PowerShell en tant qu'administrateur et exécutez la commande suivante : « Install-WindowsFeature -Name Web-IP-Security »

Cette commande revient à installer la fonctionnalité suivante dans IIS, à partir du gestionnaire de serveur :



Restreindre l'accès à l'ECP d'Exchange

Ouvrez la console de gestion d'IIS et déroulez la section "Sites". Ici, cliquez sur "Default Web Site" (1), puis sur "ecp" (2) afin d'accéder à Restrictions par adresse IP et domaine.

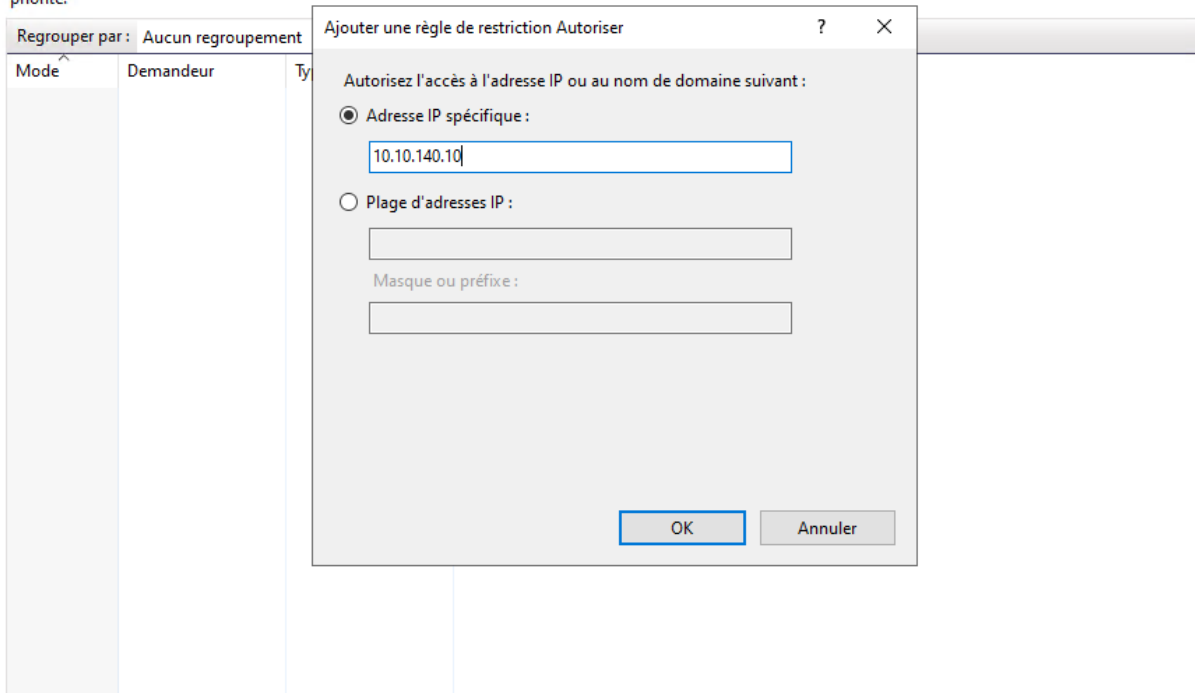


Dans la section qui s'ouvre, cliquez sur "Ajouter une entrée d'autorisation" pour ajouter une nouvelle autorisation. L'objectif ici est d'indiquer quel est la machine ou le sous-réseau autorisé à accéder au Centre d'administration Exchange. Il est possible d'ajouter plusieurs règles d'autorisation. Dans cet exemple, j'autorise les connexions à ECP depuis la machine VP-EXCHANGE "10.10.140.10". Quand c'est fait, validez avec "OK".



Restrictions par adresse IP et domaine

Utilisez cette fonction pour refuser ou octroyer l'accès au contenu Web en fonction des adresses IP et des noms de domaine. Définissez les restrictions par ordre de priorité.



Une fois que votre règle est définie (c'est modifiable par la suite), cliquez sur "Modifier les paramètres de fonction" afin de modifier l'action à appliquer pour les clients non autorisés. Par défaut, c'est autorisé, donc nous devons inverser ce comportement. Choisissez "Refuser" et pour l'action à réaliser, choisissez "Abandonner" pour couper la connexion avec le client qui tente de se connecter. Validez avec "OK".



Restrictions par adresse IP et domaine

Utilisez cette fonction pour refuser ou octroyer l'accès au contenu Web en fonction des adresses IP et des noms de domaine. Définissez les restrictions par priorité.

Regrouper par : Aucun regroupement		
Mode	Demandeur	Type d'entrée
Autoriser	10.10.140.10	Local

Modifier les paramètres de restriction IP et de...

Accès pour les clients non spécifiés :

Refuser

☐ Activer les restrictions de nom de domaine

☐ Activer le mode proxy

Refuser le type d'action :

Abandonner

OK Annuler

Pour finir, cliquez sur "Default Web Site" à gauche puis à droite sur le bouton "Redémarrer" pour redémarrer le site IIS dans le but d'appliquer la modification.

Pages and Controls Providers Session State SMTP E-mail

Logging MIME Types Modules Output Caching Request Filtering SSL Settings URL Rewrite

Actions

Explore Edit Permissions...

Edit Site

Bindings... Basic Settings...

View Applications View Virtual Directories

Manage Website

Restart Start Stop

À partir d'un client autorisé, l'accès au Centre d'administration Exchange doit fonctionner normalement. Tandis qu'à partir d'un client non autorisé, une erreur doit s'afficher, comme ceci

Désolé, impossible d'accéder à cette page.

Il semble que la page Web de <https://webmail.vdb-pro.fr/ecp> rencontre peut-être des problèmes ou qu'elle ait été déplacée définitivement vers une nouvelle adresse web.

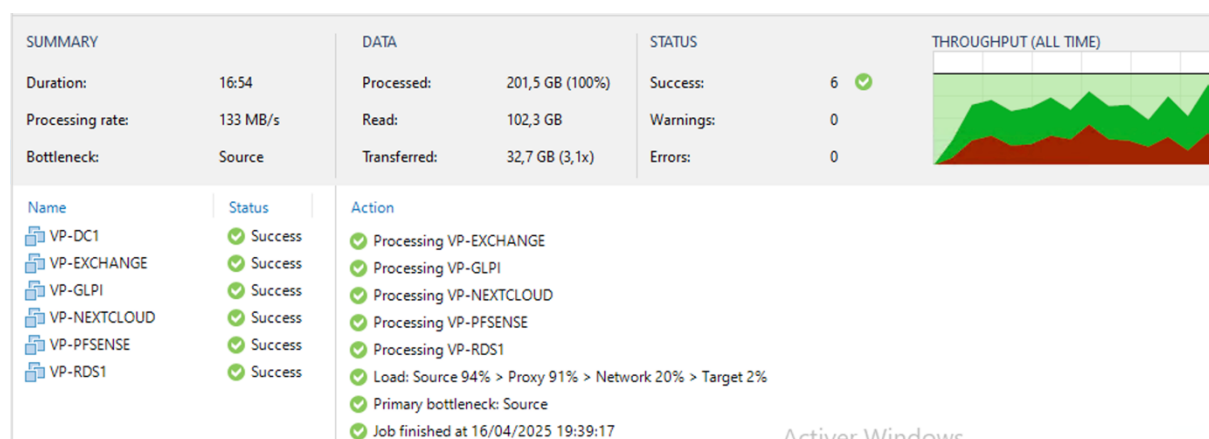
Gérer le patrimoine informatique

L'infrastructure informatique de l'entreprise **vdb-pro** repose sur un recensement rigoureux et exhaustif de l'ensemble du patrimoine informatique, réalisé à l'aide d'un outil de gestion des actifs. L'**Active Directory** constitue la base centrale de cette gestion, permettant l'organisation des utilisateurs, des groupes et des machines, tandis que d'autres services essentiels, tels qu'un serveur de **sauvegarde**, sont également en place. Le serveur **Exchange 2019**, nouvellement déployé, a été intégré à ce patrimoine et enregistré comme ressource critique de l'infrastructure.

Les droits d'accès ont été configurés en fonction des **habilitations spécifiques de chaque utilisateur**. Par exemple, l'accès au **Centre d'administration Exchange (ECP)** est strictement réservé aux administrateurs, garantissant ainsi une gestion sécurisée des paramètres sensibles, tandis que les utilisateurs classiques ne disposent que des droits nécessaires à l'usage quotidien de la messagerie.

Afin d'assurer la **continuité de service** et d'être alerté en cas de dysfonctionnement, j'ai mis en place un **système de surveillance** qui envoie des notifications par e-mail en cas de panne du serveur Exchange. Cela permet une réactivité rapide en cas d'incident.

Concernant la **sauvegarde**, un **job de sauvegarde dédié** a été mis en place pour la **machine virtuelle** hébergeant le serveur Exchange, en conformité avec le **plan de sauvegarde** de l'entreprise. Des **tests de restauration** ont été effectués avec succès afin de valider l'intégrité des sauvegardes et la capacité de reprise en cas de sinistre.



Enfin, un **système de supervision** permet de détecter et de signaler les **écarts par rapport aux règles d'utilisation des ressources numériques**, assurant un respect constant des politiques de sécurité et un usage conforme aux bonnes pratiques internes.

Développer la présence en ligne de l'organisation

L'image de l'entreprise **vdb-pro** est conforme aux attentes et soigneusement valorisée à travers une infrastructure numérique fiable, professionnelle et sécurisée. Le déploiement du serveur de messagerie Exchange participe pleinement à cette image en offrant un service de communication moderne, stable et conforme aux standards professionnels.

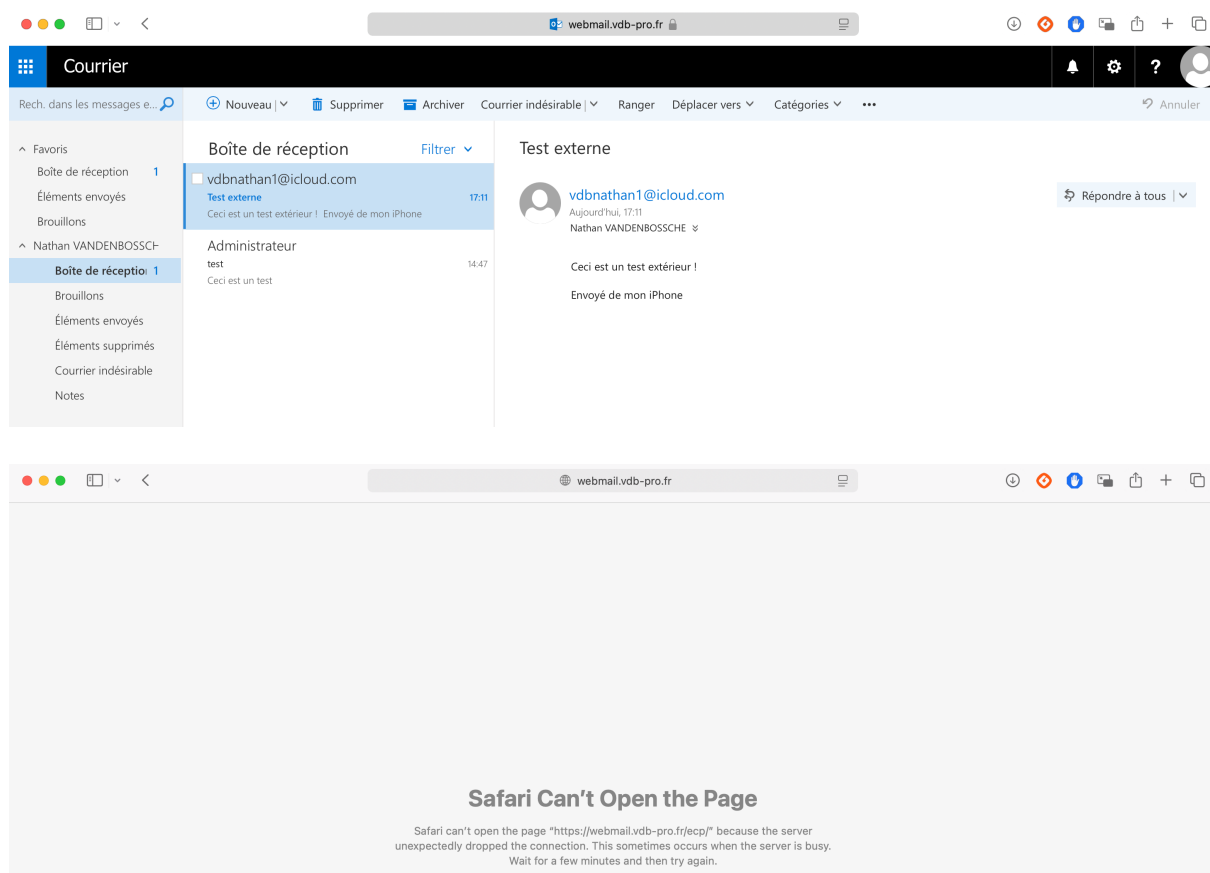
Les **enjeux économiques liés à l'image** sont clairement identifiés, notamment en ce qui concerne la confiance des partenaires et clients dans la qualité des services proposés.

La **visibilité des services en ligne**, notamment grâce au **Webmail sécurisé (OWA)**, est satisfaisante et permet aux utilisateurs d'accéder facilement aux services de messagerie, que ce soit depuis l'intérieur ou l'extérieur de l'entreprise.

De plus, les **adresses mail professionnelles des collaborateurs** sont utilisées de manière stratégique pour renforcer l'image et la cohérence de l'entreprise. Elles sont intégrées dans les **signatures mail**, ce qui contribue à véhiculer une identité visuelle professionnelle et homogène. Certaines adresses spécifiques, comme **contact@vdb-pro.fr**, sont également publiées sur le **site web officiel**, renforçant ainsi la **présence en ligne** de vdb-pro et facilitant les échanges avec les clients, partenaires ou prospects. Cette démarche améliore la visibilité de l'entreprise tout en inspirant confiance et crédibilité.

Partie 2 – Validation

Pour valider ce projet, je peux confirmer que mon serveur Exchange est correctement mis en place. Il est sécurisé à travers des règles de pare-feu strictes, garantissant la protection des flux entrants et sortants. Un certificat SSL valide a été installé, assurant ainsi la sécurité des connexions au serveur. L'accès Webmail (OWA) fonctionne parfaitement, permettant aux utilisateurs de se connecter en toute sécurité depuis n'importe quel appareil. De plus, un contrôle d'accès strict a été mis en place pour le Centre d'administration d'Exchange. En restreignant l'accès à ce centre aux administrateurs uniquement via le serveur VP-EXCHANGE, j'ai renforcé la sécurité contre les accès non autorisés. Enfin, les services de messagerie, tant pour l'envoi que la réception de mails, qu'ils soient internes ou externes, sont pleinement opérationnels, garantissant ainsi un service de messagerie fiable et sécurisé pour l'entreprise.



Conclusion

La solution de messagerie Exchange a été correctement déployée, offrant ainsi un environnement de communication sécurisé et fiable pour tous les utilisateurs de l'entreprise. Les résultats attendus ont été atteints, avec un service de messagerie entièrement fonctionnel, accessible et sécurisé, permettant à l'entreprise de répondre à ses besoins de communication électronique à court et long terme.

Partie 3 – Veille technologique

Dans le cadre de la mise en place de mon serveur de messagerie Exchange, j'ai réalisé une veille technologique approfondie pour me tenir informé des dernières innovations et solutions alternatives susceptibles d'améliorer l'efficacité et la sécurité de la solution déployée. Cette veille m'a permis d'explorer diverses options disponibles sur le marché, ainsi que de suivre les mises à jour proposées par Microsoft, notamment les **Cumulative Updates (CU)** pour Exchange Server.

Les **Cumulative Updates (CU)** jouent un rôle crucial dans l'optimisation des performances et la correction de vulnérabilités. Chaque CU apporte des améliorations fonctionnelles et de sécurité, et il est essentiel de suivre les nouvelles versions afin de garantir que le serveur Exchange reste à jour et sécurisé. Les Cumulative Updates sont publiés régulièrement et contiennent des correctifs importants pour des problèmes de performance, de stabilité et de sécurité. En outre, je me suis assuré d'utiliser la dernière CU pour garantir une sécurité infaillible.

Dans le cadre de ma veille, j'ai également exploré des **solutions alternatives** à Microsoft Exchange, telles que **Zimbra** et **Grommunio**, qui offrent des fonctionnalités similaires en matière de messagerie, de calendrier et de contacts. Ces solutions open-source ou basées sur des modèles de licences plus flexibles peuvent constituer des options intéressantes, en fonction des besoins spécifiques de l'entreprise.

Enfin, ma veille a inclus la surveillance des **meilleures pratiques de cybersécurité** liées à Exchange, telles que l'utilisation d'authentification multi-facteurs (MFA) pour protéger les connexions des utilisateurs, l'analyse des logs de sécurité pour détecter des comportements suspects, et l'intégration de solutions anti-spam et anti-phishing pour renforcer la sécurité du service de messagerie que j'envisagerai de mettre en place prochainement.

Organiser son développement professionnel

Mon **environnement d'apprentissage personnel** est structuré autour d'un laboratoire virtuel comprenant plusieurs machines virtuelles (Exchange, Active Directory, serveur de sauvegarde, etc.), me permettant de tester, configurer et valider des solutions sans impacter l'environnement de production. Cet espace est essentiel pour renforcer mes compétences techniques tout en expérimentant en toute sécurité.

Je mène également une **veille technologique régulière**, avec pour objectifs de **suivre les évolutions des mises à jour cumulatives (CU) d'Exchange**, repérer les **nouveautés et meilleures pratiques** dans le domaine de la messagerie et de la cybersécurité, et d'identifier les **alternatives potentielles** comme Zimbra ou Microsoft 365. J'utilise des sources fiables telles que les blogs officiels de Microsoft